ANTENNA GROUPING FOR GENERAL DISCRIMINATORY CHANNEL ESTIMATION

Juan Bezanilla and Javier Vía

Department of Communications Engineering, University of Cantabria, Spain
jbr54@alumnos.unican.es, jvia@gtas.dicom.unican.es

ABSTRACT

Discriminatory channel estimation emerges as a promising method of not only increasing the secrecy rates in conventional wiretap channels, but also providing a valuable tool for solving the authentication problem. In this paper, we revisit the discriminatory channel estimation method by Chang et al. and propose a generalization to the challenging scenario in which the number of antennas at the legitimate receiver equals or exceeds those of the transmitter. The proposed method is based on the simple idea of dividing the receiver antennas into smaller groups. However, the direct application of previous approaches would result into security problems due to the multiple observations of the eavesdropper, and therefore the transmission system needs to be designed taking this fact into account. The performance of the proposed technique is illustrated by means of some numerical examples, which clearly show the feasibility of discriminatory channel estimation even in the case of systems with more antennas at the receiver side.

Index Terms— Discriminatory channel estimation (DCE), multiple-input multiple-output (MIMO), physical layer security,

I. INTRODUCTION

The use of wireless communications has increased in the last years due to the amazing achievements in terms of reliability and data rate. Unfortunately, the broadcast nature of these communications makes extremely easy the interception of (maybe encrypted) data, which suggests the need of improvements in terms of security. In particular, physical layer security methods address the security problem [1] without imposing any restriction on the computing power of potential attackers, thus providing information-theoretically secure communications. This promising paradigm has triggered many interesting works on the application of physical layer security techniques [2]–[6].

This paper focuses on Discriminatory Channel Estimation (DCE), which is based on the discrimination between a legitimate receiver (Bob) and an eavesdropper (Eve), by taking into account the quality of their channel estimates. Thus DCE can be seen as a promising tool for improving the secrecy rates in conventional wiretap channels, where the degradation of the channel state information (CSI) at the eavesdropper is expected to result in additional opportunities for the legitimate pair (Alice and Bob) [3]. Moreover, DCE also emerges as a key technique for addressing authentication problems, where the quality of the channel estimates can be very helpful in order to identify potential attackers.

Previous DCE approaches include the work by Chang et al. who proposed a multistage training-based channel estimation scheme in [4]. In the first stage, a preliminary estimation of Bob's channel is obtained. In the following stages Bob sends back his estimate, which is iteratively refined, while artificial noise (AN) is superimposed in the null space of Bob's channel to degrade the estimates at the eavesdropper. Moreover, in order to reduce the overhead, Chang et al. proposed other design based on a two-way training method [7], in which both transmitter and receiver transmit pilots. Recently, Yang et al. proposed another two-way training method [8], which uses the whitening matrix of the channel between the legitimate receiver and the transmitter. However, the previous techniques require a number of antennas at the transmitter side larger than the number of antennas at Bob's, due to the need of a null space for superimposing AN.

In this paper, we focus on the original DCE technique in [4] with only two training stages, and remove the assumption on the number of antennas at Alice. In particular, we propose a general method which is based on the grouping of Bob's antennas and the transmission of AN in the null-subspace of each group. This simple idea results in a far from trivial design due to the availability of several training signals at the eavesdropper. Therefore, following a conservative approach, we assume an optimal fusion of the signals at the eavesdropper, and design the transmission scheme in order to provide accurate estimates of the legitimate channel, while guaranteeing a sufficiently poor performance of the eavesdropper channel estimator.

II. PROBLEM STATEMENT AND PROPOSED SCHEME

We consider the traditional wiretap system model [2] in Fig. 1, consisting on three wireless MIMO nodes: a transmitter Alice who wish to establish a communication with a legitimate receiver Bob, while an eavesdropper Eve is trying to tap the transmission. The number of antennas at each node is N_A, N_B and N_E respectively.

There are two stages of transmission:

This work has been supported by the Spanish Government, Ministerio de Ciencia e Innovación, under project RACHEL (TEC2013-47141-C4-3-R).

978-1-4673-7686-0/15/$31.00 ©2015 IEEE

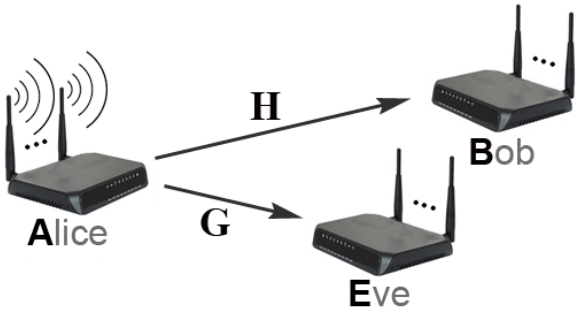


Fig. 1: Considered scenario. MIMO wiretap channel.

- In the first stage, and analogously to [4], only training sequences are transmitted.
- In the second stage, the antennas at Bob's are considered in smaller independent groups, and the stage is divided in as many turns as groups has been formed. In each turn, Alice injects artificial noise on the null-subspace of the corresponding channel group. In this manner, and without affecting Bob's, the channel estimates at Eve's are seriously degraded.

Let us finally point out that the proposed scheme can be seen as a generalization of the technique in [4]. In particular, when the size of groups is equal to N_B, the proposed scheme reduces to the technique in [4] and is able to cover the case with $N_A > N_B$.

II-A. First Stage: Conventional Training

The first stage, which takes T_0 channel uses, simply consists of the transmission of the training sequence $\mathbf{X}_0 \in \mathbb{C}^{T_0 \times N_A}$. Thus, the signals received by Bob and Eve are

$$\begin{aligned} \textbf{Bob: } & \mathbf{Y}_0 = \mathbf{X}_0\mathbf{H} + \mathbf{W}_0 \\ \textbf{Eve: } & \mathbf{Z}_0 = \mathbf{X}_0\mathbf{G} + \mathbf{V}_0 \end{aligned}$$

where the channel and noise matrices are defined in Table I. Likewise, the training matrix $\mathbf{X}_0$ is defined as

$$\mathbf{X}_0 = \sqrt{\frac{P_0 T_0}{N_A}}\mathbf{C}_0 \tag{1}$$

where P_0 is the training signal power in the first stage, and $\mathbf{C}_0 \in \mathbb{C}^{T_0 \times N_A}$ is a training matrix satisfying $\mathbf{C}_0^H\mathbf{C}_0 = \mathbf{I}_{N_A}$.

From its received signal $\mathbf{Y}_0$, Bob obtains a preliminary channel estimate of $\mathbf{H}$, denoted by $\hat{\mathbf{H}}_0 \triangleq \mathbf{H} + \Delta\mathbf{H}_0$, which is sent back to the transmitter. By applying the LMMSE criterion, $\hat{\mathbf{H}}_0$ is given by

$$\hat{\mathbf{H}}_0 = \sigma_H^2\mathbf{X}_0^H\left(\sigma_H^2\mathbf{X}_0\mathbf{X}_0^H + \sigma_w^2\mathbf{I}_{T_0}\right)^{-1}\mathbf{Y}_0. \tag{2}$$

$\mathbf{H} \in \mathbb{C}^{N_A \times N_B}$	MIMO channel from Alice to Bob. The elements of $\mathbf{H}$ are random circular uncorrelated variables, with zero mean and variance equal to σ_H^2.
$\mathbf{G} \in \mathbb{C}^{N_A \times N_E}$	MIMO channel from Alice to Eve. The elements of $\mathbf{G}$ are random circular uncorrelated variables, with zero mean and variance equal to σ_G^2.
$\mathbf{W}_0 \in \mathbb{C}^{T_0 \times N_B}$	AWGN matrix at Bob in the first stage, with variance equal to σ_w^2.
$\mathbf{V}_0 \in \mathbb{C}^{T_0 \times N_E}$	AWGN matrix at Eve in the first stage, with variance equal to σ_v^2.

Table I: Definition of channel and noise matrices.

Analyzing the error $\Delta\mathbf{H}_0$ we can obtain the correlation matrix

$$\begin{aligned} E\left\{\Delta\mathbf{H}_0(\Delta\mathbf{H}_0)^H\right\} &= N_B\left(\frac{1}{\sigma_H^2}\mathbf{I}_{N_A} + \frac{P_0T_0}{N_A\sigma_w^2}\mathbf{C}_0^H\mathbf{C}_0\right)^{-1} \\ &= N_B\left(\frac{1}{\sigma_H^2} + \frac{P_0T_0}{N_A\sigma_w^2}\right)^{-1}\mathbf{I}_{N_A} \end{aligned} \tag{3}$$

and therefore, the normalized MSE (NMSE) of the preliminary channel is given by

$$\text{NMSE}_B^0 = \frac{\text{Tr}\left(E\left\{\Delta\mathbf{H}_0(\Delta\mathbf{H}_0)^H\right\}\right)}{N_AN_B} = \left(\frac{1}{\sigma_H^2} + \frac{P_0T_0}{N_A\sigma_w^2}\right)^{-1}. \tag{4}$$

II-B. Second Stage: Artificial Noise and Training Signals

Given the channel estimate $\hat{\mathbf{H}}_0$, Alice can design the training sequence of the second stage, superimposing AN to the training matrix $\mathbf{X}_1$. In particular, and unlike [4], Bob's antennas are divided into independent groups of N_{rx} antennas, being $N_{\text{rx}} < N_A$. Accordingly, we define the number of turns in which this stage is divided, n_{turn}, as well as the length of the training matrix in each turn, T_1^{turn}. Thus, assuming for notational simplicity that N_B is a multiple of N_{rx},[1] we have

$$n_{\text{turn}} = \frac{N_B}{N_{\text{rx}}}, \qquad T_1^{\text{turn}} = \frac{T_1}{n_{\text{turn}}}. \tag{5}$$

In each of these turns, Alice transmits a signal with AN in the null subspace of the channel to the corresponding N_{rx} receiving antennas. At the end of the two stages, the signals received by Bob are

$$\mathbf{Y} = (\bar{\mathbf{C}} + \bar{\mathbf{A}})\mathbf{H} + \underbrace{\begin{bmatrix} \mathbf{W}_0 \\ \mathbf{W}_1 \\ \vdots \\ \mathbf{W}_{n_{\text{turn}}} \end{bmatrix}}_{\bar{\mathbf{W}}}, \tag{6}$$

[1] The generalization to the case of $\frac{N_B}{N_{\text{rx}}} \notin \mathbb{N}$ is straightforward.

with

$$\bar{\mathbf{C}} = \begin{bmatrix} \sqrt{\frac{P_0 T_0}{N_A}}\mathbf{C}_0 \\ \sqrt{\frac{P_1 T_1}{N_A n_{\text{turn}}}}\mathbf{C}_{1,1} \\ \vdots \\ \sqrt{\frac{P_1 T_1}{N_A n_{\text{turn}}}}\mathbf{C}_{1,n_{\text{turn}}} \end{bmatrix}, \quad \bar{\mathbf{A}} = \begin{bmatrix} \mathbf{0} \\ \mathbf{A}_1 \mathbf{N}^H_{\hat{H}_0,1} \\ \vdots \\ \mathbf{A}_{n_{\text{turn}}} \mathbf{N}^H_{\hat{H}_0,n_{\text{turn}}} \end{bmatrix}, \tag{7}$$

where $\mathbf{C}_{1,m} \in \mathbb{C}^{T_1^{\text{turn}} \times N_A}$ is a unitary training matrix, and P_1 is the power allocated to the training signals of the entire second stage. Hence, $\frac{P_1}{n_{\text{turn}}}$ is the power corresponding to each turn. $\mathbf{A}_m \in \mathbb{C}^{T_1^{\text{turn}} \times (N_A - N_{\text{rx}})}$ is the AN matrix with variance σ_A^2, and $\mathbf{N}_{\hat{H}_0,m} \in \mathbb{C}^{N_A \times (N_A - N_{\text{rx}})}$ is the null subspace of the m-th group of receiving antennas.

Finally, defining $\mathbf{w} = \text{vec}(\bar{\mathbf{W}})$ and $\mathbf{h} = \text{vec}(\mathbf{H})$, the vectorization of (6) yields

$$\mathbf{y} = (\mathbf{I}_{N_B} \otimes \bar{\mathbf{C}})\mathbf{h} + (\mathbf{I}_{N_B} \otimes \bar{\mathbf{A}})\hat{\mathbf{h}}_0 + (\mathbf{I}_{N_B} \otimes \bar{\mathbf{A}})\Delta\mathbf{h} + \mathbf{w}, \tag{8}$$

where the term $(\mathbf{I}_{N_B} \otimes \bar{\mathbf{A}})\hat{\mathbf{h}}_0 \neq 0$ due to the fact that $\mathbf{N}_{H_0}$ is only orthogonal to the space defined by the group of N_{rx} antennas used in its respective turn. Moreover, let us point out that the first and second terms are uncorrelated due to the independence between $\bar{\mathbf{C}}$ and $\bar{\mathbf{A}}$.

III. COVARIANCE MATRIX STRUCTURE AND FINAL CHANNEL ESTIMATES

This section provides the final channel estimates, which require the careful analysis of the involved covariance and cross-covariance matrices.

III-A. Covariance matrix structure

From (8), it is easy to write

$$\mathbf{C}_{hy} = \sigma_H^2 \left(\mathbf{I}_{N_B} \otimes \bar{\mathbf{C}}^H\right) \tag{9}$$

$$\begin{aligned} \mathbf{C}_{yy} =& \sigma_H^2 (\mathbf{I}_{N_B} \otimes \bar{\mathbf{C}}\bar{\mathbf{C}}^H) + \sigma_w^2 \mathbf{I}_{N_B(T_0+T_1)} \\ &+ E\left\{ \left((\mathbf{I}_{N_B} \otimes \bar{\mathbf{A}})\hat{\mathbf{h}}_0\right) \left((\mathbf{I}_{N_B} \otimes \bar{\mathbf{A}})\hat{\mathbf{h}}_0\right)^H \right\} \\ &+ E\left\{ \left((\mathbf{I}_{N_B} \otimes \bar{\mathbf{A}})\Delta\mathbf{h}\right) \left((\mathbf{I}_{N_B} \otimes \bar{\mathbf{A}})\Delta\mathbf{h}\right)^H \right\}, \end{aligned} \tag{10}$$

where the two last terms of $\mathbf{C}_{yy}$ require a more detailed analysis. In particular, the term

$$E\left\{ \left((\mathbf{I}_{N_B} \otimes \bar{\mathbf{A}})\hat{\mathbf{h}}_0\right) \left((\mathbf{I}_{N_B} \otimes \bar{\mathbf{A}})\hat{\mathbf{h}}_0\right)^H \right\} \tag{11}$$

models the effect of the AN on the antennas not belonging to the group for which it was designed. Thus, defining

$$\mathbf{f} = \left((\mathbf{I}_{N_B} \otimes \bar{\mathbf{A}})\hat{\mathbf{h}}_0\right) = \left[\mathbf{f}_1^T, \mathbf{f}_2^T, \ldots, \mathbf{f}_{N_B}^T\right]^T \tag{12}$$

we have that $\mathbf{f}_m \in \mathbb{C}^{(T_0+T_1)\times 1}$ is given by

$$\mathbf{f}_m = \bar{\mathbf{A}}\hat{\mathbf{h}}_{0,m} = \begin{bmatrix} \mathbf{0}_{T_0 \times 1} \\ \mathbf{A}_1 \mathbf{N}^H_{\hat{H}_0,1} \hat{\mathbf{h}}_{0,m} \\ \mathbf{A}_2 \mathbf{N}^H_{\hat{H}_0,2} \hat{\mathbf{h}}_{0,m} \\ \vdots \\ \mathbf{A}_{n_{\text{turn}}} \mathbf{N}^H_{\hat{H}_0,n_{\text{turn}}} \hat{\mathbf{h}}_{0,m} \end{bmatrix}, \tag{13}$$

where $\hat{\mathbf{h}}_{0,m}$ is the m-th column of $\hat{\mathbf{H}}_0$, that is, the preliminary estimate of the multiple-input single-output (MISO) channel from Alice to the m-th receive antenna. Here, it is important to note that the first T_0 entries are zero due to the absence of AN in the first stage. Moreover, among the n_{turn} vectors with length T_1^{turn} corresponding to each group of antennas, exactly N_{rx} of them will be zero due to the orthogonality between the AN and the channel of the corresponding group of antennas. Hence, the covariance matrix $\mathbf{C}_{ff}$, whose structure is illustrated in Figure 2a, consists of N_{rx}^2 matrices given by

$$E\left\{\mathbf{f}_{m_1}\mathbf{f}_{m_2}^H\right\} = \begin{bmatrix} \mathbf{0}_{T_0 \times T_0} & \mathbf{0}_{T_0 \times T_1} \\ \mathbf{0}_{T_1 \times T_0} & \mathbf{M}_{m_1,m_2} \end{bmatrix}, \tag{14}$$

where $m_1, m_2 = 1, 2, \ldots, n_{\text{turn}}$, and $\mathbf{M}_{m_1,m_2}$ is a block-diagonal matrix where the n-th block of the diagonal is given by

$$\mathbf{B}_n^f = \sigma_A^2 (N_A - N_{rx}) \text{Tr}\left(\mathbf{N}^H_{\hat{H}_{0,n}} \hat{\mathbf{h}}_{0,m_1} \hat{\mathbf{h}}^H_{0,m_2} \mathbf{N}_{\hat{H}_{0,n}}\right) \mathbf{I}_{T_1/N_B}, \tag{15}$$

with $n = 1, 2, \ldots, N_B$. In words, matrix $\mathbf{C}_{ff}$ models spurious effects (not present in the original method in [4]) due to the inner products between the projections (onto the estimated null subspace of each antenna group) of a pair of MISO channel estimates.

The analysis of the last term in (10) is simpler and follows the lines in [4]. In particular, defining

$$\mathbf{k} = ((\mathbf{I}_{N_B} \otimes \bar{\mathbf{A}})\Delta\mathbf{h}) = \left[\mathbf{k}_1^T, \mathbf{k}_2^T, \ldots, \mathbf{k}_{N_B}^T\right]^T, \tag{16}$$

we have

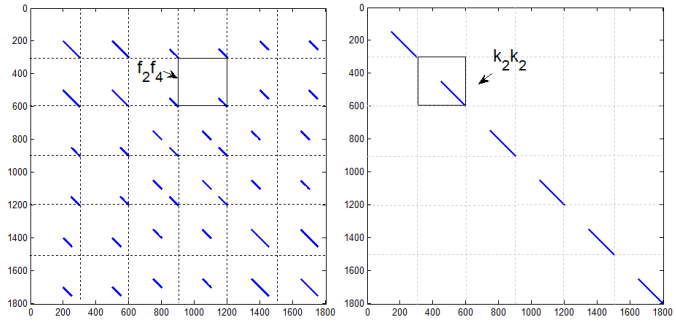
$$\mathbf{k}_m = \begin{bmatrix} \mathbf{0}_{T_0 \times 1} \\ \mathbf{A}_1 \mathbf{N}^H_{\hat{H}_0,1} \Delta\mathbf{h}_m \\ \mathbf{A}_2 \mathbf{N}^H_{\hat{H}_0,2} \Delta\mathbf{h}_m \\ \vdots \\ \mathbf{A}_{n_{\text{turn}}} \mathbf{N}^H_{\hat{H}_0,n_{\text{turn}}} \Delta\mathbf{h}_m \end{bmatrix}. \tag{17}$$

where $\Delta\mathbf{h}_m$ represents the error in the preliminary estimate of the m-th MISO channel.

Analogously to the previous case, $\mathbf{C}_{kk}$ (Figure 2b) is formed by N_{rx}^2 matrices $E\left\{\mathbf{k}_{m_1}\mathbf{k}_{m_2}^H\right\}$ with the same structure as (14). However, in this case the expectation will be null for $m_1 \neq m_2$, whereas for $m_1 = m_2$ we have block-diagonal matrices with the n-th block given by

$$\mathbf{B}_n^k = \sigma_A^2 (N_A - N_{\text{rx}})^2 N_B \text{NMSE}_B^0 \mathbf{I}_{T_1/N_B} \tag{18}$$

with $n = 1, 2, \ldots, N_B$.



(a) (b)

Fig. 2: Structure of covariance matrices. Example with $N_A = 4, N_B = 6, N_E = 5, N_{\text{rx}} = 2$, $T_0 = T_1 = 150$ (a) Matrix $\mathbf{C}_{ff}$, (b) Matrix $\mathbf{C}_{kk}$

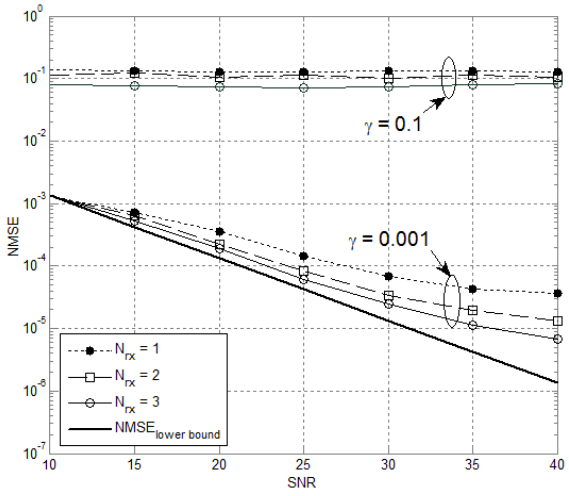


Fig. 3: NMSE performance in function of N_{rx} ($N_A = 4, N_B = 6, N_E = 5$).

III-B. Final Channel Estimates

Given the covariance and cross-covariance matrices, the final estimate of the legitimate channel is

$$\hat{\mathbf{h}}_1 = \mathbf{C}_{hy}\mathbf{C}_{yy}^{-1}\mathbf{y}. \tag{19}$$

In the case of Eve, we have a similar result for the preliminary channel estimate

$$\hat{\mathbf{G}}_0 = \sigma_G^2\mathbf{X}_0^H\left(\sigma_G^2\mathbf{X}_0\mathbf{X}_0^H + \sigma_v^2\mathbf{I}_{T_0}\right)^{-1}\mathbf{Z}_0. \tag{20}$$

and the NMSE after the first stage can be computed through the error matrix $\Delta\mathbf{G} = \hat{\mathbf{G}}_0 - \mathbf{G}$ as in eq. (4), obtaining

$$\text{NMSE}_E^0 = \left(\frac{1}{\sigma_G^2} + \frac{P_0T_0}{N_A\sigma_v^2}\right)^{-1}. \tag{21}$$

However, in the second stage Eve has to modify her estimate to take into account the channel training strategy. In this stage, the covariance and cross-covariance matrices at Eve's are computed following the lines in the previous subsection. Thus, $\mathbf{C_{gz}}$ is equivalent to (9), whereas $\mathbf{C_{zz}}$ is given by the sum of the first two terms of (10), related to data training and AWGN noise matrices, and a term involving the product between AN and the channel estimate $\hat{\mathbf{G}}$. Unlike Bob's case, the terms in the diagonal of this last term are not zero because the AN is not orthogonal to $\mathbf{G}$. As a result, Eve's estimates are obtained as

$$\hat{\mathbf{G}} = N_E\sigma_G^2\bar{\mathbf{C}}^H\left(N_E\sigma_G^2\bar{\mathbf{C}}\bar{\mathbf{C}}^H + \mathbf{R}_{\bar{V}}\right)^{-1}\mathbf{Z} \triangleq \mathbf{G} + \Delta\mathbf{G}. \tag{22}$$

where

$$\mathbf{R}_{\bar{V}} = \begin{bmatrix} N_E\sigma_v^2\mathbf{I}_{T_0} & \mathbf{0} \\ \mathbf{0} & N_E\left((N_A - N_{\text{rx}})\sigma_A^2\sigma_G^2 + \sigma_v^2\right)\mathbf{I}_{T_1} \end{bmatrix}. \tag{23}$$

Finally, due to the independence between the AN subspaces and the eavesdropper channel $\mathbf{G}$, the estimate at Eve's can be seen as a simple average of the estimates in each turn. Hence, the minimum NMSE achievable at Eve is $\frac{\gamma}{n_{\text{turn}}}$, where γ is the limit imposed to each Eve's estimate [4].

IV. SIMULATION RESULTS

The performance of the proposed technique is illustrated in this section by means of some numerical results. Only scenarios with $N_B \geq N_A$ are represented, thus focusing on the gap left by the original technique proposed in [4]. In all the simulations the transmitter (Alice) have four antennas, Bob has six antennas, and Eve has five antennas ($N_A = 4$, $N_B = 6$, $N_E = 5$). We consider i.i.d Rayleigh channels $\mathbf{H}$ and $\mathbf{G}$ constant along the whole training phase. Training sequence lengths are assumed equal in both stages $T_0 = T_1 = 150$, where T_1 refers to the whole second stage, which is later divided into n_{turn} turns. The minimum Eve's achievable NMSE is defined as γ, which is a lower bound imposed on the NMSE of Eve. The average transmission power is 30 dBm ($P_{\text{ave}} = 1$), P_0, P_1 and σ_A are designed according to the power allocation scheme in [4], with an optimization problem solved by a simple one-dimensional line search. The SNR of the channels is defined as

$$\text{SNR}_B = \frac{E\left\{\|\mathbf{X}_0\mathbf{H}\|_F^2\right\} + E\left\{\|\mathbf{X}_1\mathbf{H}\|_F^2\right\}}{\sum_{k=0}^{n_{\text{turn}}} E\left\{\|\mathbf{W}_k\|_F^2\right\}} = \frac{1}{\sigma_w^2} \tag{24}$$

$$\text{SNR}_E = \frac{E\left\{\|\mathbf{X}_0\mathbf{G}\|_F^2\right\} + E\left\{\|\mathbf{X}_1\mathbf{G}\|_F^2\right\}}{\sum_{k=0}^{n_{\text{turn}}} E\left\{\|\mathbf{V}_k\|_F^2\right\}} = \frac{1}{\sigma_v^2}. \tag{25}$$

Additionally, all our results are compared with the best NMSE performance achievable by Bob in a transmission without AN. This NMSE is given by

$$\text{NMSE}_{\text{lower bound}} = \left(\frac{1}{\sigma_H^2} + \frac{P_{\text{ave}}(T_0 + T_1)}{N_A\sigma_w^2}\right)^{-1}. \tag{26}$$

Figure 3 shows the NMSE of the channel estimate at Bob's as a function of SNR for different values of N_{rx}. In particular, for $\gamma = 0.1$ the NMSE of the legitimate receiver is similar to the best NMSE achieved in [4] (considering two-stages and satisfying $N_A > N_B$). However, for $\gamma = 0.001$, the NMSE obtained is close to $\text{NMSE}_{\text{lower bound}}$, which is

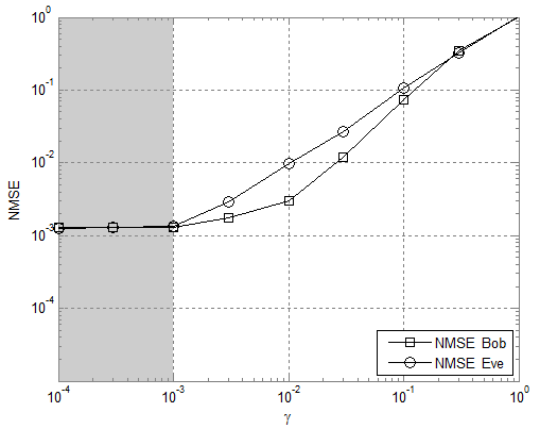


Fig. 4: NMSE performance in function of γ for $N_A = 4, N_B = 6, N_E = 5$, SNR $= 10$dB

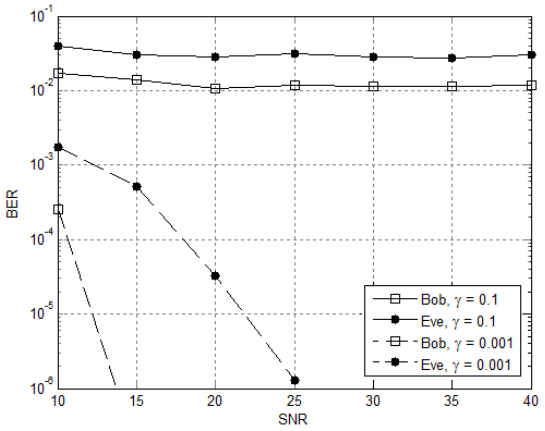


Fig. 5: BER performance in function of SNR for $N_A = 4, N_B = 6, N_E = 5$

worthwhile since training sequence is divided into only two stages. Here, we must point out that although these results seem to suggest that the performance improves with the size of the antenna groups, we have corroborated with other experiments that this is not always the case, which is a good motivation for a future study.

Figure 4 shows the NMSE performance as a function of γ for a low SNR value (10dB) and for the largest feasible antenna group size. We can see in the figure that when $\gamma < 10^{-3}$ (shaded zone of the figure), the limit imposed to the eavesdropper is so low that Alice does not need to transmit AN. That is, the proposed technique reduces to conventional channel training. Higher SNRs has been studied, observing that in this case, Alice always needs to transmit AN in order to degrade Eve's estimate. Therefore, with high SNRs the advantage provided by the proposed scheme is more noticeable.

Figure 5 shows the Bit Error Rate (BER) achieved by Bob and Eve as a function of SNR for different values of γ. The simulation is based on the transmission of uncoded QPSK symbols and zero forzing equalization (channel inversion by means of the pseudoinverse). As can be seen, Bob reaches a lower BER than Eve in all considered scenarios, which supports the idea of exploiting the proposed approach to increase the achievable secrecy rate.

V. CONCLUSIONS

This paper extends the idea of discriminatory channel estimation to the general case in which the number of antennas at the legitimate receiver is not necessarily lower than that of the transmitter. The basic idea, which consists in the transmission of artificial noise on the null subspaces of the channels to different subgroups of antennas, results in far from trivial structures on the covariance matrices for the linear minimum mean square error estimators. However, the careful processing of the received signals allows us to ensure that the legitimate pair can take advantage of the training sequence design, thus guaranteeing an improved channel estimation performance with respect to the eavesdropper. The promising results of the proposed scheme have been illustrated by means of several simulation examples. Future research lines include the optimal selection of the antenna group size.

VI. REFERENCES

[1] M. Bloch and J. Barros, "Physical-layer security: From information theory to security engineering," Cambridge Univ Pr., 2011.

[2] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[3] S. Ray, M. Mdard, and L. Zheng, "On noncoherent MIMO channels in the wideband regime. capacity and reliability," *IEEE Trans. Information Theory*, vol. 53, no. 6, pp. 1983–2009, June 2007.

[4] T.-H. Chang, W.-C. Chiang, Y.-W. Peter Hong, and C.-Y. Chi, "Training sequence design for discriminatory channel estimation in wireless MIMO systems," *IEEE Trans. Signal Processing*, vol. 58, no. 12, pp. 6223–6237, December 2010.

[5] S. Van Vaerenbergh, Ó. González, J. Vía, and I. Santamaría, "Physical layer authentication based on channel response tracking using Gaussian processes," *ICCASP*, 2014.

[6] J. Vía, "Robust secret key capacity for the MIMO induce source model," *ICCASP*, 2014.

[7] C.-W. Huan, T.-H. Chang, Y.-W. Peter Hong, and X. Zhou, "Two-way training for discriminatory channel estimation in wireless MIMO systems," *IEEE Trans. Signal Processing*, vol. 61, no. 10, pp. 2724–2738, May 2013.

[8] J. Yang, S. Xie, X. Zhou, R. Yu, and Y. Zhang, "A semiblind two-way training method for discriminatory channel estimation in MIMO systems," *IEEE Trans. Communications*, vol. 62, no. 7, pp. 2400–2410, July 2014.